#4
10f3

Attorney Docket No. 42P10855

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Patent Application of:

Michael Ripley, et al.

Application No. 09/823,423

Filed: March 29, 2001

For: **METHOD AND SYSTEM FOR PROVIDING BUS ENCRYPTION BASED ON CRYPTOGRAPHIC KEY EXCHANGE**

Examiner: Lee, Chi Chung

Art Unit: 2135

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Applicant submits, in triplicate, the following Appeal Brief pursuant to 37 C.F.R. § 1.192 for consideration by the Board of Patent Appeals and Interferences. Applicant also submits herewith a check in the amount of $330.00 to cover the cost of filing the opening brief as required by 37 C.F.R. § 1.17(c). Please charge any additional amount due or credit any overpayment to deposit Account No. 02-2666.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

Michael S. Ripley and Brendan S. Traw, the inventors named in the application, assigned his rights to that disclosed in the subject application through an assignment recorded March 29, 2001 (011676/0238) to Intel Corporation, of Santa Clara, California. Thus, as the owner at the time the brief is being filed, Intel Corporation, of Santa Clara, California is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences that will directly affect or be directly affected by or having a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-26 are pending in the present application. The Examiner has rejected all pending claims. Applicant hereby appeals the rejection of all the pending claims.

IV. STATUS OF AMENDMENTS

No amendment has been filed subsequent to the Final Office Action having a mailing date of January 9, 2004.

V. SUMMARY

A system is disclosed for protecting data transmitted over a bus from unauthorized copying and replaying. (Specification, paragraph 16, lines 1-19). The system includes an encryption subsystem to encrypt the content read from storage medium prior to transmitting the data over a bus connecting a storage device to a host device. (Specification, paragraph 12, lines 1-4). The system also includes a decryption subsystem to decrypt the data supplied from the storage device. (Specification, paragraph 13, lines 1-3). The encryption subsystem encrypts data accessed from a storage medium using an encryption bus key prior to transmitting the encrypted data via a data bus. (Specification, paragraph 15, lines 6-14). The encryption bus key is derived based on a key distribution data block, a device key assigned to the encryption subsystem and a nonce generated by a number generator. (Specification, paragraph 14, lines 1-16). The decryption subsystem is coupled to the data bus to decrypt the encrypted data received over the

data bus using a decryption bus key derived based on at least a portion of the key distribution data block, at least one device key assigned to the decryption subsystem and the nonce generated by the number generator. (Specification, paragraph 14, lines 1-16).

VI. ISSUES

The issue involved in this appeal is as follows:

Under 35 U.S.C. 103(a), are Claims 1-26 unpatentable over Natsume ("DVD Content Scramble System", June 1997, National Technical Report, Vol. 43, No. 3, pp. 338-342) in view of Miyauchi (U.S. Patent No. 6,272,225 B1)?

VII. GROUPING OF CLAIMS

Applicant contends that the claims can be divided into the following groups and that each group of claims is separately patentable. These groups are as follows:

Group I -- Claim 1;
Group II -- Claims 2, 6, 8, 9;
Group III -- Claim 3;
Group IV -- Claim 4;
Group V -- Claim 5;
Group VI -- Claim 7;
Group VII -- Claim 10;
Group VIII -- Claims 11, 12, 13, 16;
Group IX -- Claims 14, 15, 17;
Group X -- Claims 18 and 20; and
Group XI -- Claims 19 and 21-26.

Each claim group is deemed separately patentable for the reasons given below.

Claim 1 of Group I contains the limitations that an encryption subsystem to encrypt data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus, wherein the encryption bus key is derived based on at least a portion of the key distribution data block, at least one device key assigned to the encryption subsystem and the nonce generated by the number generator. Since Claim 1 of Group I contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 1 of Group I is separately patentable.

Claim 2 of Group II contains the limitations that a decryption subsystem coupled to the data bus to decrypt the encrypted data received over the data bus using a decryption bus key

derived based on at least a portion of the key distribution data block, at least one device key assigned to the decryption subsystem and the nonce generated by the number generator. Since Claim 2 of Group II contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 2 of Group II is separately patentable. Since Claims 6, 8 and 9 of Group II depend on Claim 2, Claims 2, 6, 8 and 9 stand or fall together.

Claim 3 of Group III contains the limitations that the encryption subsystem further comprises: [1] a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to the encryption subsystem to compute a media key; [2] a one-way function to generate the encryption bus key based on the media key and the nonce generated by the number generator; and [3] an encryption logic to encrypt data accessed from the storage medium using the encryption bus key. Since Claim 3 of Group III contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 3 of Group III is separately patentable.

Claim 4 of Group IV contains the limitations that the decryption subsystem further comprises: [1] a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to the decryption subsystem to compute a media key; [2] a one-way function to generate the decryption bus key based on the media key and the nonce generated by the number generator; and [3] a decryption logic to decrypt data transmitted over the data bus by using the decryption bus key. Since Claim 4 of Group IV contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 4 of Group IV is separately patentable.

Claim 5 of Group V contains the limitations that the data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if the data is recorded at the time of transmission, the recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by the encryption subsystem to encrypted the data transmitted over the data bus. Since Claim 5 of Group V contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 5 of Group V is separately patentable.

Claim 7 of Group VI contains the limitations that the encryption subsystem is implemented in a storage device capable of accessing data from a storage medium and the decryption subsystem is implemented in a host device capable of retrieving data from the storage

device. Since Claim 7 of Group VI contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 7 of Group VI is separately patentable.

Claim 10 of Group VII contains the limitations that the number generator is a random number generator residing within the decryption subsystem. Since Claim 10 of Group VII contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 10 of Group VII is separately patentable.

Claim 11 of Group VIII contains the limitations of [1] a storage device reading a key distribution data block from a storage medium; [2] the storage device processing at least a portion of the key distribution data block using at least one device key to compute a media key; [3] the storage device fetching a nonce generated by a number generator; [4] the storage device combining the nonce with the media key using a one-way function to generate a bus key; [5] the storage device encrypting data read from the storage medium using the bus key generated by the storage device; and [6] the storage device transmitting the encrypted data over a data bus. Since Claim 11 of Group VIII contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 11 of Group VIII is separately patentable. Since Claims 12, 13 and 16 of Group VIII depend on Claim 11, Claims 11, 12, 13, 16 stand or fall together.

Claim 14 of Group IX contains the limitations of [1] a host device reading the key distribution data block from the storage medium; [2] the host device processing at least a portion of the key distribution data block using at least one device key to compute a media key; [3] the host device fetching the nonce generated by the number generator; [4] the host device combining the media key with the nonce using a one-way function to generate a bus key; and [5] the host device decrypting the encrypted data received over the data bus using the bus key generated by the host device. Since Claim 14 of Group IX contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 14 of Group IX is separately patentable. Since Claims 15 and 17 of Group IX depend on Claim 14, Claims 14, 15 and 17 stand or fall together.

Claim 18 of Group X contains the limitations that a storage device to access a storage medium containing data and a key distribution data block, the storage device including a processing logic, a one-way function and an encryption logic, wherein the processing logic processes at least a portion of the key distribution data block using a device key assigned to the storage device to compute a media key, the one-way function combines the media key with a

nonce generated by a number generator to produce a bus key and the encryption logic encrypts the data accessed from the storage medium using the bus key prior to transmitting the encrypted data via a data bus. Since Claim 18 of Group X contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 18 of Group X is separately patentable. Since Claim 20 of Group IX depends on Claim 18, Claims 18 and 20 stand or fall together.

Claim 19 of Group XI contains the limitations that a host device coupled to the storage device via the data bus, the host device including a processing logic, a one-way function and a decryption logic, wherein the processing logic processes at least a portion of the key distribution data block using a device key assigned to the host device to compute a media key, the one-way function combines the media key with the nonce generated by the number generator to produce a bus key and the decryption logic decrypts the encrypted data received over the data bus using the bus key. Since Claim 19 of Group XI contains distinguishable limitations from the claims of other groups and also from the cited references, Claim 19 of Group XI is separately patentable. Since Claims 21-26 of Group XI depend on Claim 19, Claims 19 and 21-26 stand or fall together.

VIII. ARGUMENT

A. Overview of the Cited Art

1. Overview of Natsume

Natsume describes a copy protection system in which the contents on a DVD are encrypted by using triple-layer keys (i.e., title key, disc key, and master key) and only licensed DVD machines which comply with the CSS standards are capable of decoding and playing them back. (Natsume, page 8, lines 7-10). To prevent unauthorized copying of a copyrighted data decoded from a DVD by a DVD-ROM drive onto a hard disc, the bus authentication used by Natsume enables the DVD-ROM drive and the MPEG decoder module, which are connected via a computer bus (PC bus) to mutually authenticate that they comply with the CSS standards. (Natsume, page 12, lines 2-9). Absent from Natsume is any teaching or suggestion of deriving an encryption bus key based on at least a portion of a key distribution data block stored in a storage medium, at least one device key assigned to an encryption subsystem and a nonce generated by a number generator. Additionally, absent from Natsume is any teaching or

suggestion of using the derived encryption bus key to encrypt data accessed from a storage medium prior to transmitting the data via a data bus.

2. Overview of Miyauchi

Miyauchi describes various key recovery techniques to recover a decryption key that is used to decrypt the encrypted data. (Miyauchi, column 1, lines 5-67). The key recovery apparatus taught by Miyauchi is capable of including a key recover condition having relatively complex contents to key information without registering the key recover condition in a third-party organization. (Miyauchi, column 2, lines 2-7). Absent from Miyauchi is any teaching or suggestion of deriving an encryption bus key based on at least a portion of a key distribution data block stored in a storage medium, at least one device key assigned to an encryption subsystem and a nonce generated by a number generator. Additionally, absent from Miyauchi is any teaching or suggestion of using the derived encryption bus key to encrypt data accessed from a storage medium prior to transmitting the data via a data bus.

B. Group I: Rejection of Claim 1 Under 35 U.S.C. § 103(a) as Being Unpatentable over Natsume in View of Miyauchi

The Examiner rejects Claims 1-26 under 35 U.S.C. 103(a) as being unpatentable over Natsume in view of Miyauchi. The Examiner bears the burden of supporting a *prima facie* conclusion of obviousness. To establish prima facie obviousness, the Examiner must show that the cited references when combined teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination must be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). As will be shown below, the Examiner has failed to meet the burden of shown how the combination of prior art teaches or suggests all of the limitations recited in Applicant's claims. Applicant, therefore, requests that the obviousness rejections to all claims be withdrawn.

Claim 1 recites an encryption subsystem that encrypts data accessed from a storage medium using a encryption bus key prior to transmitting the encrypted data via a data bus. The claimed encryption bus key is derived based on, among other things, the key distribution data block contained in the storage medium and the nonce generated by a number generator.

In rejecting Claim 1, the Examiner asserts that "Natsume discloses a system comprising: an encryption subsystem [see figure 2] to encrypt data accessed from a storage medium containing a key distribution data block [i.e. master key 7, see Figure 2] using an encryption bus key (i.e. title key) prior to transmitting the encrypted data [see page 8 lines 18-21] via a data bus (i.e. PC bus 7, see Figure 5). The Examiner's analysis of Claim 1 is believed to be inaccurate. Particularly, in rejecting Claim 1, the Examiner equates what is shown in Figure 2 of Natsume as an encryption subsystem to encrypt data accessed from a storage medium prior to transmitting the encrypted data via a data bus. However, Figure 2 of Natsume in no way teaches or suggests an encryption subsystem to encrypt data accessed from a storage medium prior to transmitting the encrypted data via a data bus. Instead, Figure 2 of Natsume shows a block diagram for encrypting data prior to storing the data on a storage medium. As such, what is shown in Figure 2 of Natsume is wholly different from the encryption subsystem claimed in Claim 1.

Additionally, in rejecting Claim 1, the Examiner equates a "title key" of Natsume as an encryption bus key as set forth in Claim 1. However, the "title key" taught by Natsume does not serve to encrypt data accessed from a storage medium prior to transmitting the encrypted data via a data bus as set forth in Claim 1. Rather, Natsume discloses that the "title key" is used to descramble scrambled AV data on a disc (see page 11, lines 1-3 of Natsume). The "title key" of Natsume may be used to scramble data before storing the data on the disc. However, there is nothing in Natsume that teaches or suggests that the "title key" may be used to encrypt data accessed from a storage medium prior to transmitting the data via a data bus.

Generally, Claim 1 recites an encryption subsystem to encrypt data accessed from a storage medium prior to transmitting the data via a data bus. This protects the data transmitted over the bus from unauthorized copying and replaying. To the contrary, Figure 2 of Natsume (referred by the Examiner as being equivalent to the claimed encryption subsystem) describes a system for scrambling data before storing the data on a disc. Consequently, Natsume fails to teach or suggest an encryption subsystem to encrypt data accessed from a storage medium using an encryption bus key prior to transmitting the encryption data via a data bus, as set forth in Claim 1. Moreover, Natsume also fails to teach or suggest deriving an encryption bus key based on [1] a nonce generated by a number generator, [2] at least a portion of a key distribution data block and [3] at least one device key assigned to an encryption subsystem, as set forth in Claim 1. Miyauchi does not cure this deficiency.

Furthermore, Applicant respectfully asserts that the Examiner has failed to meet the burden of proof to establish a *prima facie* obviousness rejection under 35 U.S.C. § 103(a) based upon the lack of motivation to combine the references. In the case of *In re Rouffet*, 149 F.3d 1350 (Fed. Cir. 1998), the Federal Circuit specifically set forth the requirements that must be met by an examiner when an obviousness rejection is made based upon a combination of references. An Examiner "must show reasons that the skilled artisan, confronted with the *same problems* as the inventor *and with no knowledge of the claimed invention*, would select the elements from the cited prior art references for combination in the manner claimed." *Id.* at 1357. Stated another way, the Federal Circuit requires that the Examiner's basis for combining the references relate to the *same* problem as that which confronted the inventor. Natsume addresses the problem of unauthorized copying of contents stored on a DVD disc. Miyauchi addresses the drawbacks associated with conventional key recovery techniques. One of the problems that the claimed invention relates to overcoming conventional techniques that fail to protect data transmitted over a bus from unauthorized copying and replaying. Because the references relied upon by the Examiner do not relate to the *same* problem confronted by the inventors, Applicant respectfully asserts that the Examiner has impermissibly engaged in hindsight analysis in order to support its obviousness rejection. For this reason alone, the Examiner has failed to adequately set forth an obviousness rejection under 35 U.S.C. § 103(a).

For all the foregoing reasons, Applicant submits that the rejection of Claim 1 under 35 U.S.C. § 103(a) as being obvious over Natsume in view of Miyauchi is in error.

C. Group II: Rejection of Claims 2, 6, 8 and 9 Under 35 U.S.C. § 103(a) as Being Unpatentable over Natsume in View of Miyauchi

Claim 2 is dependent on patentably independent Claim 1, as discussed above, and those arguments are hereby incorporated regarding Claim 2. Additionally, Claim 2 is independently nonobvious as none of the cited references disclose or suggest a decryption subsystem coupled to a data bus to decrypt the encrypted data received over the data bus using a decryption bus key derived based on at least a portion of the key distribution data block, at least one device key assigned to the decryption subsystem and the nonce generated by the number generator.

In rejecting Claim 2, the Examiner asserts that Natsume teaches "a decryption subsystem [see figure 5] coupled to said data bus to decrypt data received over the data bus using an

decryption bus key derived based on at least a portion of the key distribution data block (i.e. master key), at least one device key (i.e., disc key) assigned to said encryption subsystem [see page 10 lines 1-16]." In this regard, the Examiner equates the "disc key" 11 shown in Figure 5 of Natsume as the "device key" claimed in Claim 2. Claim 2 requires that the device key is assigned to the decryption subsystem. To the contrary, the disc key 11 illustrated in Figure 5 of Natsume is derived from the encrypted disc key set 1 stored on the DVD disc. As such, Natsume fails to teach deriving a decryption bus key based on, among other things, at least one device key assigned to the decryption subsystem, as claimed in Claim 2. Miyauchi does not cure this deficiency. Additionally, because the references (Natsume and Miyauchi) relied upon by the Examiner do not relate to the *same* problem confronted by the inventors, Applicant respectfully asserts that the Examiner has impermissibly engaged in hindsight analysis in order to support the obviousness rejection of Claim 2. Therefore, the rejection of claim 2 is erroneous.

Claims 6, 8 and 9 are dependent on patentably independent Claim 1, as discussed above, and those arguments are hereby incorporated regarding Claims 6, 8 and 9. At least for this reason, Applicant respectfully submits that Claims 6, 8 and 9 are allowable.

D. Group III: Rejection of Claim 3 Under 35 U.S.C. § 103(a) as Being Unpatentable over Natsume in View of Miyauchi

Claim 3 is dependent on patentably independent Claim 1, as discussed above, and those arguments are hereby incorporated regarding Claim 3. Additionally, Claim 3 is independently nonobvious as none of the cited references disclose or suggest a one-way function to generate the encryption bus key based on the media key and the nonce generated by the number generator.

In rejecting Claim 3, the Examiner admits that Natsume fails to disclose an one-way function to generate the encryption bus key based on the media key and a nonce generated by the number generator. The Examiner then asserts that the hashing unit 100 shown in Figure 1 of Miyauchi is equivalent to the one-way function as claimed in Claim 3.

In Claim 3, the one-way function is used to generate the encryption bus key based on the media key and the nonce generated by the number generator. To the contrary, the hashing unit 100 shown in Figure 1 of Miyauchi has nothing to do with the random number Kr generated by the random generator 400. Accordingly, the hashing unit 100 shown in Figure 1 of Miyauchi,

which the Examiner equates as being the one-way function, does not generate an output based on a nonce generated by a number generator as claimed in Claim 3.

Additionally, because the references (Natsume and Miyauchi) relied upon by the Examiner do not relate to the *same* problem confronted by the inventors, Applicant respectfully asserts that the Examiner has impermissibly engaged in hindsight analysis in order to support the obviousness rejection of Claim 3. Therefore, the rejection of claim 3 is erroneous.

E. Group IV: Rejection of Claim 4 Under 35 U.S.C. § 103(a) as Being Unpatentable over Natsume in view of Miyauchi

Claim 4 is dependent on patentably independent Claim 2, as discussed above, and those arguments are hereby incorporated regarding Claim 4. Additionally, Claim 4 is independently nonobvious as none of the cited references disclose or suggest a one-way function to generate the decryption bus key based on the media key and the nonce generated by the number generator.

In rejecting Claim 4, the Examiner admits that Natsume fails to disclose an one-way function to generate the decryption bus key based on the media key and a nonce generated by the number generator. The Examiner then asserts that the hashing unit 100 shown in Figure 1 of Miyauchi is equivalent to the one-way function as claimed in Claim 4.

In Claim 4, the one-way function is used to generate the decryption bus key based on the media key and the nonce generated by the number generator. To the contrary, the hashing unit 100 shown in Figure 1 of Miyauchi has nothing to do with the random number Kr generated by the random generator 400. Accordingly, the hashing unit of Miyauchi, which the Examiner equates as being the one-way function does not generate an output based on a nonce generated by a number generator as claimed in Claim 4.

Additionally, because the references (Natsume and Miyauchi) relied upon by the Examiner do not relate to the *same* problem confronted by the inventors, Applicant respectfully asserts that the Examiner has impermissibly engaged in hindsight analysis in order to support the obviousness rejection of Claim 4. Therefore, the rejection of claim 4 is erroneous.

F. Group V: Rejection of Claim 5 Under 35 U.S.C. § 103(a) as Being Unpatentable over Natsume in View of Miyauchi

Claim 5 is dependent on patentably independent Claim 1, as discussed above, and those arguments are hereby incorporated regarding Claim 5. Additionally, Claim 5 is independently nonobvious as none of the cited references disclose or suggest using a bus key to encrypt the data transmitted over a data bus such that if the data is recorded at the time of transmission, the recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by the encryption subsystem to encrypted the data transmitted over the data bus.

In rejecting Claim 5, The Examiner has not carried the burden the patent law imposes on the Examiner to present a *prima facie* case of obviousness by failing to point out where the claimed features of Claim 5 are found within the cited references. In the Office Actions, the Examiner fails to point out where features claimed in Claim 5 are found in either Natsume or Miyauchi. Applicant likewise cannot find any such teaching or suggestion.

The Examiner is obligated to examine every claim both independent and dependent. It is not Applicant's responsibility to show that a claim is patentable until the Examiner first makes out a prima facie case of unpatentability. Since the Examiner has not carried the initial burden of presenting a *prima facie* case of obviousness, the rejection of Claim 5 is erroneous.

G. Group VI: Rejection of Claim 7 Under 35 U.S.C. § 103(a) as Being Unpatentable over Natsume in View of Miyauchi

Claim 7 is dependent on patentably independent Claim 2, as discussed above, and those arguments are hereby incorporated regarding Claim 7. Additionally, Claim 7 is independently nonobvious as none of the cited references provide an encryption subsystem, which is implemented in a storage device capable of accessing data from a storage medium and a decryption subsystem, which is implemented in a host device capable of retrieving data from the storage device.

In rejecting the base claim (i.e., Claim 1) of Claim 7, the Examiner asserted that Figure 2 of Natsume is equivalent to the encryption subsystem claimed in Claim 1. However, the device shown in Figure 2 of Natsume is not a storage device capable of accessing data from a storage medium. As such, the content scramble device shown in Figure 2 of Natsume, which the

Examiner equates as the claimed encryption subsystem, is not implemented in a storage device capable of accessing data from a storage medium, as required by Claim 7. Therefore, the rejection of claim 7 is erroneous.

H. Group VII: Rejection of Claim 10 Under 35 U.S.C. § 103(a) as Being Unpatentable over Natsume in View of Miyauchi

Claim 10 is dependent on patentably independent Claim 2, as discussed above, and those arguments are hereby incorporated regarding Claim 10. Additionally, Claim 10 is independently nonobvious as none of the cited references teaches or suggests a random number generator residing within the decryption subsystem.

In rejecting Claim 10, The Examiner has not carried the burden the patent law imposes on the Examiner to present a *prima facie* case of obviousness by failing to point out where the claimed features of Claim 10 are found within the cited references. In the Office Actions, the Examiner fails to point out where features claimed in Claim 10 are found in either Natsume or Miyauchi. Since the Examiner has not carried the initial burden of presenting a *prima facie* case of obviousness, the rejection of Claim 10 is erroneous.

I. Group VIII: Rejection of Claims 11, 12, 13 and 16 Under 35 U.S.C. § 103(a) as Being unpatentable over Natsume in View of Miyauchi

Claim 11 recites a method comprising: [1] a storage device reading a key distribution data block from a storage medium; [2] the storage device processing at least a portion of said key distribution data block using at least one device key to compute a media key; [3] the storage device fetching a nonce generated by a number generator; [4] the storage device combining said nonce with said media key using a one-way function to generate a bus key; [5] the storage device encrypting data read from the storage medium using the bus key generated by the storage device; and [6] the storage device transmitting the encrypted data over a data bus.

In rejecting Claim 11, the Examiner merely asserts that Claims 11-17 recites steps that correspond to the functions of the elements of the apparatus Claims 1-10, and thus Claims 11-17 are rejected for the reasons without pointing out where all of the features claimed in Claim 11 are taught by the combination of Natsume and Miyauchi. For example, Applicant submits that the combination of Natsume and Miyauchi fails to teach or suggest the storage device combining the

nonce generated by a number generator and the media key using a one-way function to generate a bus key, as set forth in Claim 11. As noted above, the hashing unit 100 shown in Figure 1 of Miyauchi, which the Examiner equates as being the one-way function, does not generate an output based on a nonce generated by a number generator, much less combine a nonce generated by a number generator with a media key to generate a bus key, as required by Claim 11.

The Examiner is obligated to examine every claim both independent and dependent. Here the Examiner has not met that obligation by failing to point out how the combination of Natsume and Miyauchi teaches a storage device combining a nonce generated by a number generator and a media key using a one-way function to generate a bus key. As such, the rejection of Claim 11 is erroneous.

Claims 12, 13 and 16 are dependent on patentably independent Claim 11, as discussed above, and those arguments are hereby incorporated regarding Claims 12, 13 and 16. At least for this reason, Applicant respectfully submits that Claims 12, 13 and 16 are allowable.

J. Group IX: Rejection of Claims 14, 15 and 17 Under 35 U.S.C. § 103(a) as Being Unpatentable over Natsume in View of Miyauchi

Claim 14 is dependent on patentably independent Claim 11, as discussed above, and those arguments are hereby incorporated regarding Claim 14. Additionally, Claim 14 is independently nonobvious as none of the cited references teaches or suggests a host device combining a media key with a nonce using a one-way function to generate a bus key, as recited by Applicant.

In rejecting Claim 14, the Examiner merely asserts that Claims 11-17 recites steps that correspond to the functions of the elements of the apparatus Claims 1-10, and thus Claims 11-17 are rejected for the reasons without pointing out where all of the features claimed in Claim 14 are taught by the combination of Natsume and Miyauchi. For example, Applicant submits that the combination of Natsume and Miyauchi fails to teach or suggest the host device combining the media key with the nonce using a one-way function to generate a bus key, as claimed in Claim 14. As noted above, the hashing unit 100 shown in Figure 1 of Miyauchi, which the Examiner equates as being the one-way function, does not generate an output based on a nonce generated by a number generator, much less combine a nonce generated by a number generator with a media key to generate a bus key, as required by Claim 14.

The Examiner is obligated to examine every claim both independent and dependent. Here the Examiner has not met that obligation failing to point out how the combination of Natsume and Miyauchi teaches a host device combining a media key with a nonce using a one-way function to generate a bus key, as recited by Applicant. As such, the rejection of Claim 14 is erroneous.

Claims 15 and 17 are dependent on patentably base Claims11 and 14, as discussed above, and those arguments are hereby incorporated regarding Claims 15 and 17. At least for this reason, Applicant respectfully submits that Claims 17 and 17 are allowable.

K. Group X: Rejection of Claims 18 and 20 Under 35 U.S.C. § 103(a) as Being Unpatentable over Natsume in View of Miyauchi

Claim 18 recites an apparatus comprising a storage device to access a storage medium containing data and a key distribution data block, the storage device including a processing logic, a one-way function and an encryption logic, wherein the processing logic processes at least a portion of the key distribution data block using a device key assigned to the storage device to compute a media key, the one-way function combines the media key with a nonce generated by a number generator to produce a bus key and the encryption logic encrypts the data accessed from the storage medium using the bus key prior to transmitting the encrypted data via a data bus.

In rejecting Claim 18, the Examiner merely asserts that Claims 18-26 have similar limitations as Claims 1-10, and thus they are rejected for the same rational without pointing out where all of the features claimed in Claim 18 are taught by the combination of Natsume and Miyauchi. For example, Applicant submits that the combination of Natsume and Miyauchi fails to teach or suggest a storage device that includes a one-way function that combines the media key with a nonce generated by a number generator to produce a bus key, as claimed in Claim 18.

The Examiner is obligated to examine every claim both independent and dependent. Here the Examiner has not met that obligation by failing to point out how the combination of Natsume and Miyauchi teaches a storage device that includes a one-way function that combines the media key with a nonce generated by a number generator to produce a bus key. As such, the rejection of Claim 18 is erroneous.

Claim 20 is dependent on patentably independent Claim 18, as discussed above, and those arguments are hereby incorporated regarding Claim 20. At least for this reason, Applicant respectfully submits that Claim 20 is allowable.

L. Group XI: Rejection of Claims 19 and 21-26 Under 35 U.S.C. § 103(a) as Being Unpatentable over Natsume in View of Miyauchi

Claim 19 is dependent on patentably independent Claim 18, as discussed above, and those arguments are hereby incorporated regarding Claim 19. Additionally, Claim 19 is independently nonobvious as none of the cited references teaches or suggests a host device having an one-way function that combines the media key with a nonce generated by a number generator to produce a bus key, as recited by Applicant.

In rejecting Claim 19, the Examiner merely asserts that Claims 18-26 have similar limitations as Claims 1-10, and thus they are rejected for the same rational without pointing out where all of the features claimed in Claim 19 are taught by the combination of Natsume and Miyauchi. The Examiner is obligated to examine every claim both independent and dependent. Here the Examiner has not met that obligation failing to point out how the combination of Natsume and Miyauchi teaches a host device having an one-way function that combines the media key with a nonce generated by a number generator to produce a bus key, as recited by Applicant. As such, the rejection of Claim 19 is erroneous.

Claims 21-26 are dependent on patentably independent Claim 19, as discussed above, and those arguments are hereby incorporated regarding Claims 21-26. At least for this reason, Applicant respectfully submits that Claims 21-26 are allowable.

IX. CONCLUSION AND RELIEF

Based on the foregoing, Applicant requests that the Board overturn the rejection of all pending claims and hold that all of the claims of the present application are allowable.

Respectfully submitted,

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP

Dated: January 26, 2004

By: _____
Walter T. Kim, Reg. No. 42,731

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF MAILING:
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on January 26, 2004

_____
Marilyn Bass January 26, 2004

X. APPENDIX

1. (Original) A system comprising:

a number generator to generate a nonce; and

an encryption subsystem to encrypt data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus, wherein said encryption bus key is derived based on at least a portion of the key distribution data block, at least one device key assigned to said encryption subsystem and the nonce generated by the number generator.

2. (Original) The system of claim 1, further comprising a decryption subsystem coupled to said data bus to decrypt said encrypted data received over the data bus using a decryption bus key derived based on at least a portion of the key distribution data block, at least one device key assigned to said decryption subsystem and the nonce generated by the number generator.

3. (Original) The system of claim 1, wherein said encryption subsystem comprises:

a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said encryption subsystem to compute a media key;

a one-way function to generate the encryption bus key based on the media key and the nonce generated by the number generator; and

an encryption logic to encrypt data accessed from said storage medium using said encryption bus key.

4. (Original) The system of claim 2, wherein said decryption subsystem comprises:

a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said decryption subsystem to compute a media key;

a one-way function to generate the decryption bus key based on said media key and the nonce generated by the number generator; and

a decryption logic to decrypt data transmitted over the data bus by using said decryption bus key.

5. (Original) The system of claim 1, wherein said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by said encryption subsystem to encrypted said data transmitted over the data bus.

6. (Original) The system of claim 2, wherein said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data.

7. (Original) The system of claim 2, wherein said encryption subsystem is implemented in a storage device capable of accessing data from a storage medium and said decryption subsystem is implemented in a host device capable of retrieving data from said storage device.

8. (Original) The system of claim 2, wherein said media key computed by the said encryption subsystem will be the same as the media key computed by the decryption subsystem provided that neither the device key assigned to the encryption subsystem nor the device key assigned to the decryption subsystem have been compromised.

9. (Original) The system of claim 2, wherein said storage medium is selected from a digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory, magnetic card and optical card.

10. (Original) The system of claim 2, wherein said number generator is a random number generator residing within said decryption subsystem.

11. (Original) A method comprising:

a storage device reading a key distribution data block from a storage medium;

the storage device processing at least a portion of said key distribution data block using at least one device key to compute a media key;

the storage device fetching a nonce generated by a number generator;

the storage device combining said nonce with said media key using a one-way function to generate a bus key;

the storage device encrypting data read from the storage medium using the bus key generated by the storage device; and

the storage device transmitting the encrypted data over a data bus.

12. (Original) The method of claim 11, wherein said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a host device that does not have access to the same nonce used by the storage device to encrypted said data transmitted over the data bus.

13. (Original) The method of claim 11, further comprising decrypting the encrypted data received over the data bus.

14. (Original) The method of claim 13, wherein said decrypting the encrypted data received over the data bus comprises:

a host device reading the key distribution data block from the storage medium;

the host device processing at least a portion of the key distribution data block using at least one device key to compute a media key;

the host device fetching the nonce generated by the number generator;

the host device combining said media key with the nonce using a one-way function to generate a bus key; and

the host device decrypting said encrypted data received over the data bus using the bus key generated by the host device.

15. (Original) The method of claim 14, further comprising:

the host device requesting a descramble key required for descrambling scrambled content from said storage device;

the storage device encrypting said descramble key read from said storage medium with said bus key generated by said storage device and sending said encrypted descramble key to the host device;

the host device decrypting said encrypted descramble key received from said storage device using said bus key generated by said host device.

the host device descrambling said decrypted data using said descramble key decrypted by said host device.

16. (Original) The method of claim 11, wherein said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data.

17. (Original) The method of claim 14, wherein said number generator is a random number generator residing within the host device.

18. (Original) An apparatus comprising:

a storage device to access a storage medium containing data and a key distribution data block, said storage device including a processing logic, a one-way function and an encryption logic, wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said storage device to compute a media key, said one-way function combines said media key with a nonce generated by a number generator to produce a bus key and said encryption logic encrypts said data accessed from said storage medium using said bus key prior to transmitting the encrypted data via a data bus.

19. (Original) The apparatus of claim 18, further comprising a host device coupled to said storage device via said data bus, said host device including a processing logic, a one-way function and a decryption logic, wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said host device to compute a media key, said one-way function combines said media key with said nonce generated by said number generator to produce a bus key and said decryption logic decrypts said encrypted data received over the data bus using said bus key.

20. (Original) The apparatus of claim 18, wherein said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a host device that does not have access to the same nonce used by said storage device to encrypted said data transmitted over the data bus.

21. (Original) The apparatus of claim 19, wherein said media key computed by the said storage device will be the same as the media key computed by the host device provided that neither the device key assigned to the storage device nor the device key assigned to the host device have been compromised.

22. (Original) The apparatus of claim 19, wherein said number generator is a random number generator residing within said host device.

23. (Original) The apparatus of claim 19, wherein said storage device is embodied in the form of a DVD drive and said host device is embodied in the form of either a DVD player or a personal computer.

24. (Original) The apparatus of claim 19, wherein said storage medium is selected from a digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory, magnetic card and optical card.

25. (Original) The apparatus of claim 19, wherein said storage medium is embodied in the form of a DVD containing scrambled content.

26. (Original) The apparatus of claim 19, wherein said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data.

120

27.00
AF
$

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application No.	09/823,423
Filing Date	March 29, 2001
First Named Inventor	Michael S. Ripley
Art Unit	2131
Examiner Name	Lee, Chi Chung
Total Number of Pages in This Submission	27
Attorney Docket Number	42390P10855

ENCLOSURES *(check all that apply)*

- [X] Fee Transmittal Form
  - [X] Fee Attached
- [ ] Amendment / Response
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
  - [ ] PTO/SB/08
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Basic Filing Fee
  - [ ] Declaration/POA
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s)
- [ ] After Allowance Communication to Group
- [ ] Appeal Communication to Board of Appeals and Interferences
- [X] Appeal Communication to Group **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [X] Other Enclosure(s) *(please identify below)*:

Return receipt postcard

Remarks

Appeal Brief submitted in triplicate

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Walter T. Kim, Reg. No. 42,731 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	Walter T. Kim
Date	January 26, 2004

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	Marilyn Bass		
Signature	Marilyn Bass	Date	01-26-04

FEE TRANSMITTAL for FY 2003

Effective 01/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($) 330.00

Complete if Known	
Application Number	09/823,423
Filing Date	March 29, 2001
First Named Inventor	Michael S. Ripley
Examiner Name	Lee, Chi Chung
Group/Art Unit	2131
Attorney Docket No.	42390P10855

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

The Commissioner is authorized to: *(check all that apply)*

☐ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) required under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES

	Extra Claims		Fee from below		Fee Paid
Total Claims		- 26 =		X =	
Independent Claims		- 3 =		X =	
Multiple Dependent				=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple Dependent claim, if not paid
1204	86	2204	43	**Reissue independent claims over original patent
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

***or number previously paid, if greater, For Reissues, see below*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920 *	1804	920 *	Requesting publication of SIR prior to Examiner action	
1805	1,840 *	1805	1,840 *	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	1,210	2255	605	Extension for reply within fifth month	
1404	330	2401	165	Notice of Appeal	330.00
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	1809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	
Other fee (specify)					

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 330.00

SUBMITTED BY

Name *(Print/Type)*	Walter T. Kim	Registration No. *(Attorney/Agent)*	42,731	Telephone	(310) 207-3800
Signature	Walter T. Kim			Date	01-26-04

Complete (if applicable)